PATENT ABSTRACTS OF JAPAN

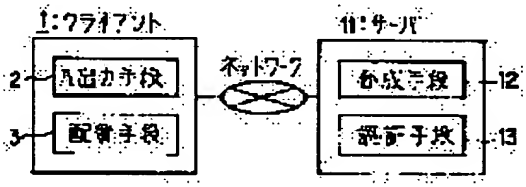
(11)Publication number : 2000-020718
(43)Date of publication of application : 21.01.2000

(51)Int.Cl. G06T 7/00
G06F 19/00

(21)Application number : 10-180935 (71)Applicant : FUJITSU LTD
(22)Date of filing : 26.06.1998 (72)Inventor : SATAKE SHUICHI

(54) CERTIFICATION SYSTEM AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent a seal from being illegally used and to detect modification of a document after checking the seal with respect to a certification device for arranging a seal image on a document by preparing a keyword based on disclosed information and document information, integrating the keyword in a bit map, arranging a seal image obtained by compositing the seal image and the bit map on a document, and extracting the arranged seal image from the received image to collate it.



SOLUTION: The certification system is provided with a 1st composite means for preparing a keyword from the document information of a document on which information related to a user and a seal image are to be arranged and incorporating the keyword in a bit map, a 2nd composite means 12 for compositing the integrated pattern with the seal image and a means 3 for arranging the seal image obtained after synthesis by the means 12 on a prescribed position of the document.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－20718
（P2000－20718A）
(43)公開日　平成12年１月21日(2000.1.21)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４５５	５Ｂ０４３
Ｇ０６Ｆ　19/00		15/30	Ｈ	５Ｂ０５５

審査請求　未請求　請求項の数６　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－180935

(22)出願日　平成10年６月26日(1998.6.26)

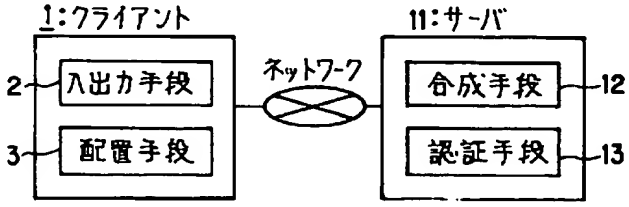
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　佐竹　修一
富山県婦負郡八尾町保内二丁目２番１　株式会社富山富士通内
(74)代理人　100089141
弁理士　岡田　守弘

Ｆターム(参考)　5B043 AA07 AA10 BA09 EA01 FA07 HA02
5B055 HA12 HB05 JJ00

(54)【発明の名称】　認証システムおよび記録媒体

(57)【要約】
【課題】　本発明は、文書に印鑑イメージを配置する認証装置に関し、秘密情報、公開情報および文書情報をもとにキーワードを作成してビットマップに組み込んだ後、印鑑イメージとビットマップを合成した印鑑イメージを文書に配置および受信文書から配置された印鑑イメージを取り出して照合し、印鑑の不正使用を防止すると共に検印後の文書の改変を検出することを目的とする。
【解決手段】　利用者に関する情報および印鑑イメージを配置しようとする文書の文書情報からキーワードを作成し、このキーワードをビットマップに組み込む第１の合成手段と、組み込んだパターンと印鑑イメージを合成する第２の合成手段と、第２の合成手段によって合成した後の印鑑イメージを文書中の所定位置に配置する手段とを備えるように構成する。

本発明のシステム構成図



【特許請求の範囲】
【請求項１】文書に印鑑イメージを配置する認証装置において、
利用者に関する情報および印鑑イメージを配置しようとする文書の文書情報からキーワードを作成し、このキーワードをビットマップに組み込む第１の合成手段と、
上記組み込んだパターンと印鑑イメージを合成する第２の合成手段と、
上記第２の合成手段によって合成した後の印鑑イメージを文書中の所定位置に配置する手段とを備えたことを特徴とする認証システム。
【請求項２】受信した文書中に配置された印鑑イメージの認証を行う認証装置において、
利用者に関する情報および受信した文書の文書情報からキーワードを作成し、このキーワードをビットマップに組み込む第１の合成手段と、
上記組み込んだパターンと印鑑イメージを合成する第２の合成手段と、
上記第２の合成手段によって合成した後の印鑑イメージと、受信した文書中から取り出した印鑑イメージとを比較して一致したときに真、不一致のときに偽と判別する手段とを備えたことを特徴とする認証システム。
【請求項３】上記利用者に関する情報として、利用者のパスワードを含む秘密情報および利用者の名前を含む公開情報としたことを特徴とする請求項１あるいは請求項２記載の認証システム。
【請求項４】上記文書の文書情報として、印鑑イメージを配置しようとする文書中の文字数を含む文書情報としたことを特徴とする請求項１から請求項３のいずれかに記載の認証システム。
【請求項５】利用者に関する情報および印鑑イメージを配置しようとする文書の文書情報からキーワードを作成し、このキーワードをビットマップに組み込む第１の合成手段と、
上記組み込んだパターンと印鑑イメージを合成する第２の合成手段と、
上記第２の合成手段によって合成した後の印鑑イメージを文書中の所定位置に配置する手段として機能させるプログラムを記録したコンピュータ読取可能な記録媒体。
【請求項６】受信した文書中に配置された印鑑イメージの認証を行う認証装置において、
利用者に関する情報および受信した文書の文書情報からキーワードを作成し、このキーワードをビットマップに組み込む第１の合成手段と、
上記組み込んだパターンと印鑑イメージを合成する第２の合成手段と、
上記第２の合成手段によって合成した後の印鑑イメージと、受信した文書中から取り出した印鑑イメージとを比較して一致したときに真、不一致のときに偽と判別する手段として機能させるプログラムを記録したコンピュータ読取可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、文書に印鑑イメージを配置する認証装置および記録媒体に関するものである。
【０００２】
【従来の技術】複数のコンピュータをネットワークを介して接続したシステムにおいて、決裁業務をグループウェアを利用して電子的に行う電子決裁システムが広く知られている。
【０００３】従来、電子決裁システムでは、印鑑データをイメージデータの形で予めサーバに保有し、パスワードの入力により特定文書の特定位置に印鑑イメージを配置し、決裁がされた旨を表すようにしていた。
【０００４】
【発明が解決しようとする課題】しかし、入力時にパスワードで認証する方法を採用していたため、検印文書毎に印鑑イメージを変えることが難しく、どの電子媒体においても同一の印鑑イメージが付加されてしまい、印鑑イメージの偽造や盗用されてしまう可能性があるという問題があった。
【０００５】更に、検印後に文書を変更された場合の確認ができないという問題もあった。本発明は、これらの問題を解決するため、秘密情報、公開情報および文書情報をもとにキーワードを作成してビットマップに組み込んだ後、印鑑イメージとビットマップを合成した印鑑イメージを文書に配置および受信文書から配置された印鑑イメージを取り出して照合し、印鑑の不正使用を防止すると共に検印後の文書の改変を検出することを目的としている。
【０００６】
【課題を解決するための手段】図１を参照して課題を解決するための手段を説明する。図１において、クライアント１は、ネットワークを介したサーバ１１と相互に通信して各種業務処理を行うものであって、ここでは、入出力手段２、および配置手段３から構成されるものである。
【０００７】入出力手段２は、パスワードや社員番号などの各種情報を入力したり、操作指示したり、結果を表示したりなどするものである。配置手段３は、印鑑イメージを文書中の所定位置に配置するものである。
【０００８】サーバ１１は、ネットワークを介してクライアント１からの要求を受信したり、要求に対する応答を返信したりなどするものであって、ここでは、合成手段１２、認証手段１３から構成されるものである。尚、合成手段１２および認証手段１３をサーバ１１に設けたが、クライアント１内に設けるようにしてもよい。
【０００９】合成手段１２は、利用者に関する情報（秘密情報および公開情報）および文書情報からキーワード

を作成し、このキーワードをビットマップに組み込んだりするものである。

【００１０】認証手段１３は、文書中から取り出した印鑑イメージと、利用者に関する情報および文書から取り出した文書情報をもとにキーワードを作成しこのキーワードをビットマップに組み込んだ印鑑イメージとを、照合して認証するものである。

【００１１】次に、動作を説明する。合成手段１２を構成する第１の合成手段が利用者に関する情報および文書の文書情報からキーワードを作成してこのキーワードをビットマップに組み込み、合成手段１２を構成する第２の合成手段が組み込んだパターンと印鑑イメージとを合成し、配置手段３が合成した後の印鑑イメージを文書中の所定位置に配置するようにしている。

【００１２】また、合成手段１２を構成する第１の合成手段が利用者に関する情報および受信した文書の文書情報からキーワードを作成してこのキーワードをビットマップに組み込み、合成手段１２を構成する第２の合成手段が組み込んだパターンと印鑑イメージとを合成し、認証手段１３が合成した後の印鑑イメージと、受信した文書中から取り出した印鑑イメージとを比較して一致したときに真、不一致のときに偽と判別するようにしている。

【００１３】これらの際に、利用者に関する情報として、利用者のパスワードを含む秘密情報および利用者の名前を含む公開情報としている。また、文書の文書情報として、印鑑イメージを配置しようとする文書中の特定文字の文字数を含む文書情報としている。

【００１４】従って、パスワードを含む秘密情報、利用者の氏名を含む公開情報および文書の文書情報をもとにキーワードを作成してビットマップに組み込んだ後、印鑑イメージとビットマップを合成した印鑑イメージを文書に配置したり、受信文書から配置された印鑑イメージを取り出して照合したりすることにより、印鑑の不正使用を防止すると共に検印後の文書の改変を検出することが可能となる。

【００１５】

【発明の実施の形態】次に、図２から図１２を用いて本発明の実施の形態および動作を順次詳細に説明する。

【００１６】図２は、本発明の概念説明図（その１）を示す。図２の（ａ）は、ビットマップ（識別データ）の作成手順例を示す。図２の（ａ－１）は、秘密情報（パスワードなど）、公開情報（検印日付けなど）および文書情報をもとにキーワードを合成する様子を示す。ここで、秘密情報は、利用者個人のみが知っているパスワードなどの秘密情報である。公開情報は、利用者の公開している情報であって、下記のものがある。

【００１７】

・社員番号
・名前
・役職
・その他

また、文書の文書情報としては、印鑑イメージを配置しようとする文書（受信した文書を含む）の文書に関する情報であって、例えば下記のようなものである。

【００１８】

・文書内文字数（総文字数）
・ひらがな文字数
・カタカナ文字数
・空白文字数
・数字文字数
・特定文字数（複数可）
・その他

これら秘密情報、公開情報および文書情報をもとに、キーワードを作成する（図１２を用いて後述する）。

【００１９】図２の（ａ－２）は、①キーワードと②ビットマップを合成し、キーワード埋め込み後の③ビットマップを生成する様子を示す。図２の（ａ－２）において、①キーワードは、図２の（ａ－１）で合成したキーワードである。

【００２０】②ビットマップは、キーワード埋め込み前の黒ベタのビットマップである。③ビットマップは、キーワード埋め込み後のビットマップである。この③ビットマップは、ここでは、①キーワードと、黒ベタの②ビットマップとをドット対応でＡＮＤ合成したものである。ここでは、黒を“１”とし、以下も同様である。尚、白を“１”とした場合には、ＯＲとなる。

【００２１】図２の（ｂ）は、検印用印鑑イメージの作成手順例を示す。図２の（ｂ）において、④検印者登録印鑑イメージは、検印者の生の登録した印鑑イメージである。

【００２２】③ビットマップは、図２の（ａ－２）のキーワード埋め込み後のビットマップである。⑤印鑑イメージは、④印鑑イメージと、③ビットマップとをＡＮＤ合成した後の印鑑イメージであって、文書中の所定位置に配置しようとする印鑑イメージである。この印鑑イメージ⑤は、キーワードを黒ベタのビットマップに埋め込み（ビット対応でＡＮＤ演算して埋め込み）、更に④印鑑イメージでＡＮＤ合成したいわば当該印鑑イメージで打ち抜いた形の印鑑イメージであり、復元は不可能な一方通行の合成を行ったものである。

【００２３】以上のようにして、秘密情報（パスワードなど）、公開情報（利用者の氏名、役職など）および文書情報（文書内の総文字数、ひらがな総文字数など）をもとにキーワードを合成し、キーワードとビットマップ（例えば黒ベタのビットマップ）を合成したキーワードを埋め込んだ③ビットマップを生成し、更に、生の④印鑑イメージでＡＮＤ演算していわば当該④印鑑イメージで打ち抜いて⑤印鑑イメージを生成し、この⑤印鑑イメージを文書中の所定位置に配置して電子捺印することに

より、秘密情報、公開情報および文書情報を非可逆的な合成を行って文書中に配置して印鑑イメージの盗用や文書の改変を防止することが可能となる。

【００２４】図３は、本発明の概念説明図（その２）を示す。これは、図２の②ビットマップが黒ベタであるのに対して、白ベタにした場合のものである。図３の（ａ）は、ビットマップ（識別データ）の作成手順例を示す。

【００２５】図２の（ａ－１）は、秘密情報（パスワードなど）、公開情報（検印日付けなど）および文書情報をもとにキーワードを合成する様子を示す。ここで、秘密情報は、利用者個人のみが知っているパスワードなどの秘密情報である。公開情報は、利用者の公開している情報であって、下記のものがある。

【００２６】
・社員番号
・名前
・役職
・その他

また、文書の文書情報としては、印鑑イメージを配置しようとする文書（あるいは受信した文書）の文書に関する情報であって、例えば下記のようなものである。

【００２７】
・文書内文字数（総文字数）
・ひらがな文字数
・カタカナ文字数
・空白文字数
・数字文字数
・特定文字数（複数可）
・その他

これら秘密情報、公開情報および文書情報をもとに、キーワードを作成する（図１２を用いて後述する）。

【００２８】図３の（ａ－２）は、①キーワードと②ビットマップを合成し、キーワード埋め込み後の③ビットマップを生成する様子を示す。図２の（ａ－２）において、①キーワードは、図２の（ａ－１）で合成したキーワードである。

【００２９】②ビットマップは、キーワード埋め込み前の白ベタのビットマップである。③ビットマップは、キーワード埋め込み後のビットマップである。この③ビットマップは、ここでは、①キーワードと、白ベタの②ビットマップとをドット対応でＯＲ合成したものである。

【００３０】図３の（ｂ）は、検印用印鑑イメージの作成手順例を示す。図３の（ｂ）において、④検印者登録印鑑イメージは、検印者の生の登録した印鑑イメージである。

【００３１】③ビットマップは、図３の（ａ－２）のキーワード埋め込み後のビットマップである。⑤印鑑イメージは、④印鑑イメージと、③ビットマップとを合成した後の印鑑イメージであって、ここでは、④印鑑イメージの外枠で③ビットマップを打ち抜き（マスクして）その内部はビット対応でＯＲ合成したものであり、文書中の所定位置に配置しようとする印鑑イメージである。この印鑑イメージ⑤は、キーワードを白ベタのビットマップに埋め込み（ビット対応でＯＲ演算して埋め込み）、更に④印鑑イメージでＯＲ合成した印鑑イメージであり、復元は不可能な一方通行の合成を行ったものである。

【００３２】以上のようにして、秘密情報（パスワードなど）、公開情報（利用者の氏名、役職など）および文書情報（文書内の総文字数、ひらがな総文字数など）をもとにキーワードを合成し、キーワードとビットマップ（白ベタのビットマップ）を合成したキーワードを埋め込んだ③ビットマップを生成し、更に、生の④印鑑イメージでＯＲ演算および印鑑イメージの外枠で打ち抜いて⑤印鑑イメージを生成し、この⑤印鑑イメージを文書中の所定位置に配置して電子捺印することにより、秘密情報、公開情報および文書情報を非可逆的な合成を行って文書中に配置して印鑑イメージの盗用や文書の改変を防止することが可能となる。

【００３３】次に、図４のフローチャートに示す順番に従い、既述した図１から図３の構成および概念を使用した本願発明の実施例について詳細に説明する。図４は、本発明の動作説明フローチャート（その１）を示す。

【００３４】図４において、Ｓ１は、社員番号を登録する。Ｓ２は、暗証番号を登録する。Ｓ３は、検印用文書情報を登録する。これらＳ１からＳ３は、例えば後述する図５の（ａ）の画面をクライアント１の表示装置上に表示し、利用者が自身の社員番号「１２３４５６７８９０」、暗証番号「＊＊＊＊＊＊＊＊」（＊は任意の英数字、記号などを表す）、検印用文書情報をキー入力あるいは画面上から選択入力する。ここで、検印用文書情報は、図５の（ａ）の画面上に示すように、文書内文字数、ひらがな文字数、かたかな文字数、空白文字数、数字文字数などの項目中から選択入力、および特定文字の文字数（複数可）を選択したときは更に右下領域にその特定文字をキー入力し、検印対象の文書中から自動採取すべき文書情報を指定する。ここで、社員番号は利用者の公開情報であり、暗証番号は利用者の秘密情報であり、検印用文書情報が文書情報である。

【００３５】Ｓ４は、名前を登録する。Ｓ５は、役職を登録する。Ｓ６は、印鑑形状を登録する。

【００３６】Ｓ７は、印鑑サイズを登録する。これらＳ４からＳ７は、例えば後述する図５の（ｂ）の画面をクライアント１の表示装置上に表示し、利用者が自身の名前「富士」、役職「開発課長」、印鑑形状「丸（日付け有）」、印鑑サイズ「１２mm」をキー入力し、サーバ１１に登録する。

【００３７】Ｓ８は、登録印鑑イメージを作成する。これは、印鑑イメージについては、スキャナーを用いて予

めあるいは同時に読み込んで作成し、サーバ１１に登録する。ここで、印鑑イメージがドロー（ベクトル）情報である場合には、スキャナは不要である。利用者のサインなどを使うときにスキャナを用いて電子化した印鑑イメージにする。

【００３８】以上によって、利用者は図５の（ａ）、（ｂ）の画面上から公開情報（利用者の社員番号、名前、役職など）、秘密情報（暗証番号など）、および印鑑イメージとその情報（印鑑形状、印鑑サイズなど）を入力してここでは、サーバ１１に登録する。

【００３９】図５は、本発明の画面例を示す。図５の（ａ）は、検印者情報の設定の画面例を示す。この画面では、図示の下記の情報を入力あるいは選択するものである。

【００４０】

・社員番号：例えば「１２３４５６７８９０」を入力

・暗証番号：例えば「＊＊＊＊＊＊＊＊＊＊」を入力

・検印用文書情報（□をチェックして選択）

□文書内文書数：

□ひらがな文字数

□かたかな文字数

□空白文字数

□数字文字数

□特定文字の文字数（複数可）：この場合には、右下ウィンドウに特定文字をキー入力

以上の項目を入力あるいは選択し、登録ボタンを押下すると、クライアント１１からネットワークを介してサーバ１１に登録されることとなる。

【００４１】図５の（ｂ）は、印鑑イメージ登録の画面例を示す。この画面では、図示の下記の情報を入力あるいは選択入力するものである。

・名前：例えば「富士」を入力

・役職：例えば「開発課長」をを入力

・印鑑形状：例えば「丸（日付け有）」をプルダウンメニューから選択

・印鑑サイズ：例えば「１２ｍｍ」を増減ボタンを押下して設定入力

・印鑑イメージ：上記データから検索されたイメージを表示

以上の項目を入力あるいは選択し、登録ボタンを押下すると、クライアント１１からネットワークを介してサーバ１１に登録されることとなる。

【００４２】図６は、本発明の動作説明フローチャート（その２）を示す。図６において、Ｓ１１は、印鑑設置領域の選択を行う。これは、利用者が後述する図７の（ａ）の表示装置の画面上に表示した文書中の検印欄を、印鑑設置領域として選択する。

【００４３】Ｓ１２は、社員番号を通知する。Ｓ１３は、暗証番号を通知する。Ｓ１４は、検印文書を送付する。これらＳ１１からＳ１４は、利用者がクライアント１の表示装置の後述する図７の（ａ）の画面上で印鑑設置領域を文書中の検印欄を指定、社員番号を入力、暗証番号を入力した後、検印文書と一緒にこれら情報をネットワークを介してサーバ１１に送付する。

【００４４】Ｓ１５は、登録印鑑イメージを検索する。これは、サーバ１１でＳ１２の社員番号、Ｓ１３の暗証番号をもとに当該利用者の登録印鑑イメージを検索して取り出す。

【００４５】Ｓ１６は、キーワードを作成する。これは、既述した図２の（ａ）、図３の（ａ）で説明したように、秘密情報（暗証番号など）、公開情報（社員番号、名前、役職など）および文書情報をもとにキーワードを作成する。

【００４６】Ｓ１７は、ビットマップを作成する。これは、Ｓ１６で作成したキーワードをビットマップに組み込んで作成する（図２の（ａ－２）、図３の（ａ－２）参照）。

【００４７】Ｓ１８は、検印用印鑑イメージを作成する。これは、Ｓ１７で作成したキーワードを埋め込んだビットマップと、印鑑イメージとを合成して検印用印鑑イメージを作成する（既述した図２の（ｂ）、図３の（ｂ）参照）。

【００４８】Ｓ１９は、検印用印鑑イメージを通知する。これは、サーバ１１がＳ１８で作成した検印用印鑑イメージをネットワークを介してクライアント１に通知する。Ｓ２０は、検印用印鑑イメージの文書内埋め込みを行う。これは、Ｓ１９でサーバ１１からクライアント１が受信した検印用印鑑イメージを、後述する例えば図７の（ｂ）のＳ１１で選択された検印の欄に配置する（埋め込む）。

【００４９】以上によって、クライント１が検印対象の文書中から検印領域の選択、公開情報（社員番号など）、秘密情報（暗証番号など）および文書情報をサーバ１１に送信し、サーバ１１がこれら情報をもとにキーワードを作成して印鑑イメージと合成して非可逆的な検印用印鑑イメージを生成し、クアイアントに送信し、クライアント１が検印対象の文書中に配置し（埋め込み）、一連の検印処理を終了する。これにより、利用者の公開情報、秘密情報、文書情報および印鑑イメージを非可逆的に合成した検印用印鑑イメージを作成して文書中に配置することで、盗用されることなく、検印後に文書が改変されても検出できる検印用印鑑イメージで文書に検印することが可能となる。

【００５０】図７は、本発明の画面例を示す。図７の（ａ）は、文書に検印するときの検印実行画面の例を示す。図７の（ａ）において、左下の検印の欄は、文書中の検印する領域として選択する領域である。

【００５１】右側の検印の実行の画面は、文書の上に表示された別ウィンドウであって、ここでは、検印の実行に必要な図示の下記の情報を入力する画面である。

・社員番号：
・暗証番号：
以上のように、検印領域の選択（検印欄を選択）、社員番号、暗証番号を入力して確認ボタンを押下すると、自動的にクライアント１からネットワークを介してサーバ１１に送信されることとなる（既述した図６のＳ１からＳ１４）。

【００５２】図７の（ｂ）は、文書に検印するときの検印実行通知画面の例を示す。ここで、左下の検印の欄には、検印用印鑑イメージが配置されている（埋め込まれている）（既述した図６の２０）。

【００５３】以上のように、選択した検印の欄に、サーバ１１から送られてきた検印用印鑑イメージを配置することで、利用者の公開情報、秘密情報、文書情報、および印鑑イメージから合成した非可逆的な検印用印鑑イメージを文書中の検印欄に自動的に配置し、検印を行うことが可能となる。

【００５４】図８は、本発明の動作説明フローチャート（その３）を示す。これは、既述したキーワードをビットマップに組み込んで作成するときの詳細フローチャートである。

【００５５】図８において、Ｓ３１は、ビットマップを作成する。ここでは、例えば既述した図２の（ａ－２）の黒ベタの②ビットマップ、あるいは図３の（ａ－２）の白ベタの②ビットマップを作成する。

【００５６】Ｓ３２は、キーワードから乱数発生用関数を作成する。これは、例えば既述した図２の（ａ－１）で作成したキーワードから乱数発生用関数を作成する（図１２参照）。

【００５７】Ｓ３３は、ピクセルデータの書換えを行う。これは、Ｓ３２で作成した乱数発生用関数をもとに、ピクセル単位にＳ３１で作成したビットマップの書換えを行い、キーワードを埋め込んだビットマップを作成する。

【００５８】以上によって、ビットマップについて、キーワードから作成した乱数をもとにピクセル単位に書換えを行い、キーワードを埋め込んだビットマップを自動作成することが可能となる。

【００５９】図９は、本発明の動作説明フローチャート（その４）を示す。図９において、Ｓ４１は、確認検印の指定を行う。これは、例えば後述する図１０の（ａ）の文書中の検印欄の印鑑イメージの検印の確認の指定を行う。

【００６０】Ｓ４２は、社員番号を通知する。Ｓ４３は、検印文書情報を通知する。Ｓ４４は、検印用印鑑イメージを通知する。

【００６１】Ｓ４５は、検印文書を送付する。これらＳ４１からＳ４５は、クライアント１の表示装置の画面上で利用者が検印対象の文書を表示し、確認する検印（印鑑イメージ）を指定し、社員番号、検印文書情報、検印用印鑑イメージ、検印文書をサーバ１１に送信する。

【００６２】Ｓ４６は、キーワードを作成する。これは、サーバ１１が、利用者の公開情報（社員番号など）、秘密情報（暗証番号など）、文書情報（文書内の総文字数など）からキーワードを作成する。

【００６３】Ｓ４７は、登録印鑑イメージを検索する。これは、社員番号と暗証番号をもとに該当する生の印鑑イメージを検索して取り出す。Ｓ４８は、確認印鑑イメージを作成する。これは、Ｓ４７で取り出した利用者の印鑑イメージ、およびＳ４６で作成したキーワードをもとに既述したようにして検印用印鑑イメージを作成する。

【００６４】Ｓ４９は、印鑑イメジーを比較する。これは、Ｓ４８で作成した検印用印鑑イメージと、Ｓ４４でクライアント１から通知を受けた検印対象の文書から取り出した印鑑イメージとをビット対応で一致するか否かを比較する。一致する場合には、検印対象の文書から取り出した印鑑イメージが真正のものと判定し、不一致の場合には、偽のものと判定する。

【００６５】Ｓ５０は、比較結果を通知する。これにより、クライアント１は、サーバ１１からＳ４９で比較した結果（真正、偽）の受け取り、文書中の印鑑イメージが真正か（後述する図１０の（ｂ）参照）、偽か（後述する図１０の（ｃ）参照）を認識できることとなる。

【００６６】以上によって、検印対象の文書中から取り出した印鑑イメージについて、当該文書の文書情報、公開情報（利用者の社員番号など）、秘密情報（暗証番号など）をもとにキーワードを作成し、当該キーワードと生の印鑑イメージとから作成した検印用印鑑イメージを比較した一致したときに真正、不一致のときに偽と判定することにより、印鑑イメージの盗用や検印後の文書の改変を検出することが可能となる。

【００６７】図１０は、本発明の画面例を示す。図１０の（ａ）は、検印確認実行画面の例を示す。これは、検印対象の文書中から検印する対象の領域として、ここでは、検印の欄を選択した指定した状態を示す。右側のウィンドウ上に選択した領域の検印を確認するメッセージが表示されているので、確認ボタンを押下すると検印処理が開示される。

【００６８】図１０の（ｂ）は、検印確認画面（正当）の例を示す。これは、検印対象の文書中の指定した検印欄の印鑑イメージについて、既述した図９のＳ４１からＳ５０による処理によって、クライアント１の表示装置の画面上に表示された、正当の場合の検印確認画面である。ここでは、「選択した領域の検印が正当（真正）です」というメッセージを表示し、検印欄の印鑑イメージが改変されていなく、かつ、検印対象の文書が改変されていない旨を表示したものである。

【００６９】図１０の（ｃ）は、検印確認画面（不当）の例を示す。これは、検印対象の文書中の指定した検印

欄の印鑑イメージについて、既述した図９のＳ４１からＳ５０による処理によって、クライアント１の表示装置の画面上に表示された、不当の場合の検印確認画面である。ここでは、「選択した領域の検印が不当（偽）です、直ちに担当部署に連絡して下さい」というメッセージを表示し、検印欄の印鑑イメージが改変、あるいは検印対象の文書が改変されている旨を表示したものである。

【００７０】図１１は、本発明の印鑑イメージテーブル例を示す。これは、サーバ１１に保存する印鑑イメージテーブルの例であって、ここでは、図示の下記の項目を対応づけて登録したものである。

【００７１】

・社員番号：
・暗証番号：
・イメージファイル：印鑑イメージ
・属性：印鑑イメージの属性（印鑑サイズ、印鑑形状など）

図１２は、本発明のキーワード組み込み説明図を示す。これは、既述した公開情報、文書情報、秘密情報をもとにキーワードを生成した後、乱数を生成するときの具体例である（図８参照）。

【００７２】図１２の（ａ）、（ｂ）は、パレットデータおよびピクセルデータの例をそれぞれ示す。これは、１６色ないし２５６色のビットマップは、通常、パレット部とピクセルデータ部を持ち、パレット部は色の数、ピクセルデータ部はビットマップを構成するドットの数分存在してその値は使用するパレットのインデックス番号である。ここで、パレットデータ内にあるデータはＲＧＢ情報であり、ピクセルデータ内にあるデータはビットマップを構成するドットが使用しているパレットの番号である。このため、パレット０が黒である場合、黒ベタのビットマップのピクセルデータの値は、全て０となる。

【００７３】図１２の（ｃ）は、パスワード（秘密情報）、検印日付け（公開情報）、文書内文字数（文書情報）の例を示す。ここでは、図示の下記の値を持つとする。

・パスワード（秘密情報）：１２３４
・検印日付け（公開情報）：９８０３０３
・文書内文字数（文書情報）：９８０３０２

図１２の（ｄ）は、キーワードの例を示す。これは、図１２の（ｃ）のパスワード、検印日付け、文書内文字数を順に並べて図示の下記の数字列をキーワードとして生成する。

【００７４】

・キーワード：１２３４９８０３０３９８０３０２

図１２の（ｅ）は、キーワードを４分割し、定数を作成する。これは、図１２の（ｄ）のキーワードを先頭から４つ飛び、第２番目から４つ飛び、第３番目から４つ飛び、第４番目から４つ飛びに図示の下記の定数１から定数４を作成する。

【００７５】

・定数１：１９００
・定数２：２８３３
・定数３：３０９０
・定数４：４３８２

図１２の（ｆ）は、３次曲線を作成する。これは、図１２の（ｅ）の定数１、２、３、４をＸの関数の定数の３次、２次、１次、定数に代入して図示の下記の３次曲線を作成する。

【００７６】

$Y=1900X^3+2833X^2+3090X+4382$

図１２の（ｇ）は、図１２の（ｆ）の３次曲線の値を２５５（２５６個目のパレットは背景の白に残しておく）で割った余りを求めて乱数を生成する様子を示す。これは、図１２の（ｆ）の式のＸにピクセルデータのインデックス値を代入して得られたＹの値をパレット数（ここでは２５６としている）で割った余りをピクセルデータに格納すれば、ビットマップにキーワードを組み込むことが可能となる。

【００７７】尚、完成したビットマップが使用するパレットの色が全て黒ならば、組み込み後も黒ベタのビットマップとなる。また、実際に使用する関数は以下のようになるため、キーワードを組み込んだビットマップからキーワードを分離することはできない。

【００７８】$Y=(1900X^3+2833X^2+3090X+4382)\%255$

ここで、Ａ％Ｂは、ＡをＢで割った際の余りを表す。

【００７９】

【発明の効果】以上説明したように、本発明によれば、パスワードを含む秘密情報、利用者の氏名を含む公開情報および文書の文書情報をもとにキーワードを作成してビットマップに組み込んだ後、印鑑イメージとビットマップを合成した印鑑イメージを文書に配置したり、受信文書から配置された印鑑イメージを取り出して照合したりする構成を採用しているため、印鑑の不正使用を防止できると共に、検印後の文書の改変を検出できる。

【図面の簡単な説明】

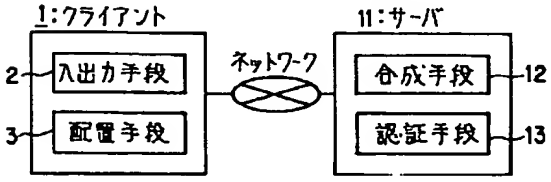
【図１】本発明のシステム構成図である。
【図２】本発明の概念説明図（その１）である。
【図３】本発明の概念説明図（その２）である。
【図４】本発明の動作説明フローチャート（その１）である。
【図５】本発明の画面例である。
【図６】本発明の動作説明フローチャート（その２）である。
【図７】本発明の画面例である。
【図８】本発明の動作説明フローチャート（その３）である。

【図９】本発明の動作説明フローチャート（その４）である。
【図１０】本発明の画面例である。
【図１１】本発明の印鑑イメージテーブル例である。
【図１２】本発明のキーワード組み込み説明図である。
【符号の説明】

１：クライアント
２：入出力手段
３：配置手段
１１：サーバ
１２：合成手段
１３：認証手段

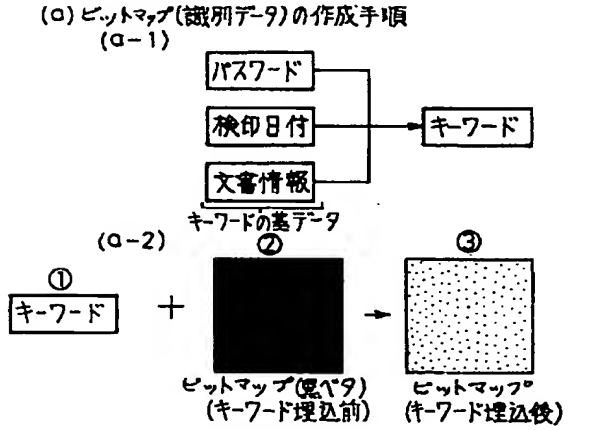
【図１】

本発明のシステム構成図



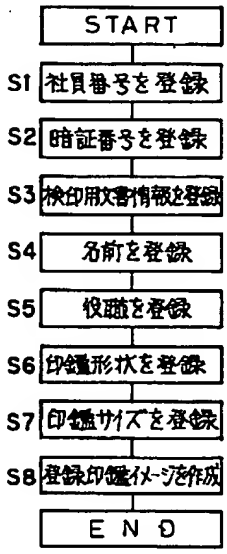
【図２】

本発明の概念説明図（その１）



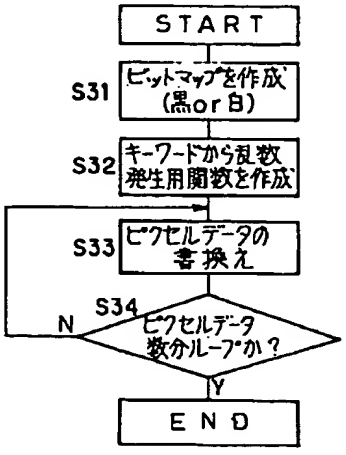
【図４】

本発明の動作説明フローチャート(その1)



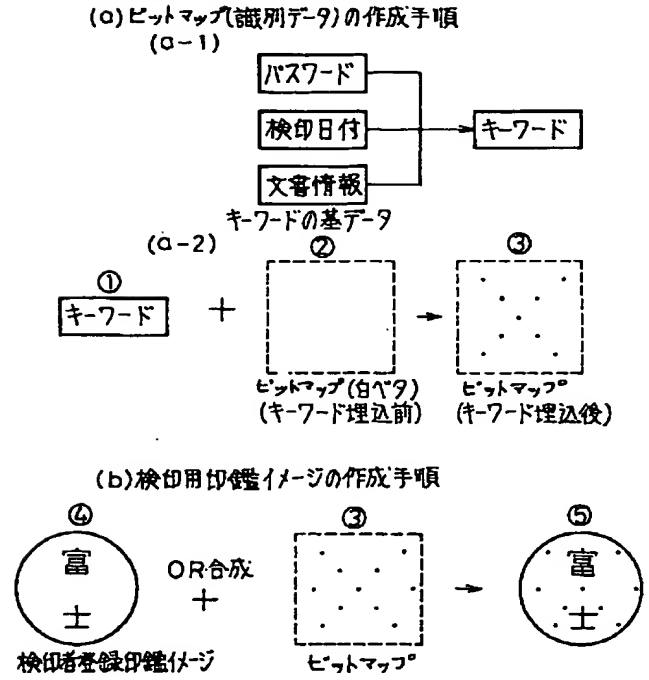
【図８】

本発明の動作説明フローチャート(その3)



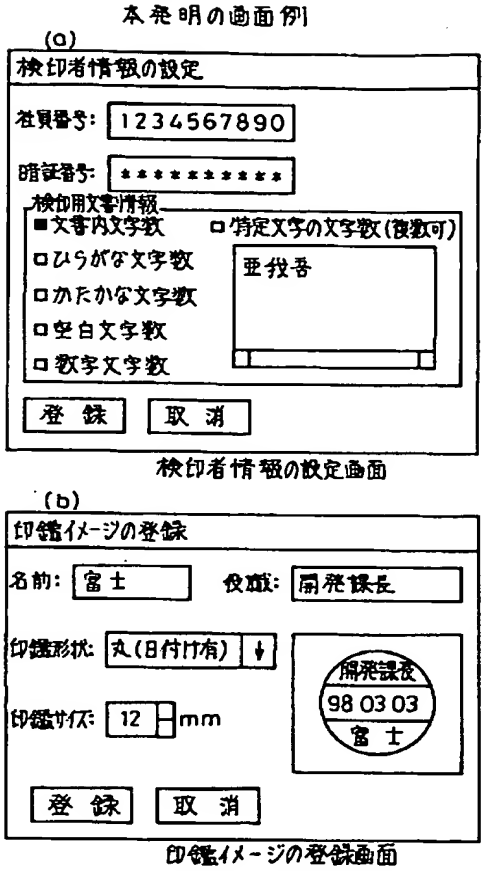
【図３】

本発明の概念説明図(その2)



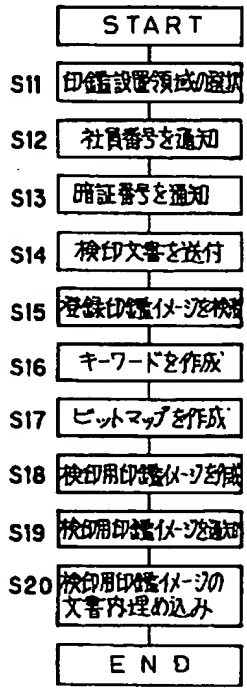
【図５】

本発明の画面例



【図６】

本発明の動作説明フローチャート(その2)



【図１１】

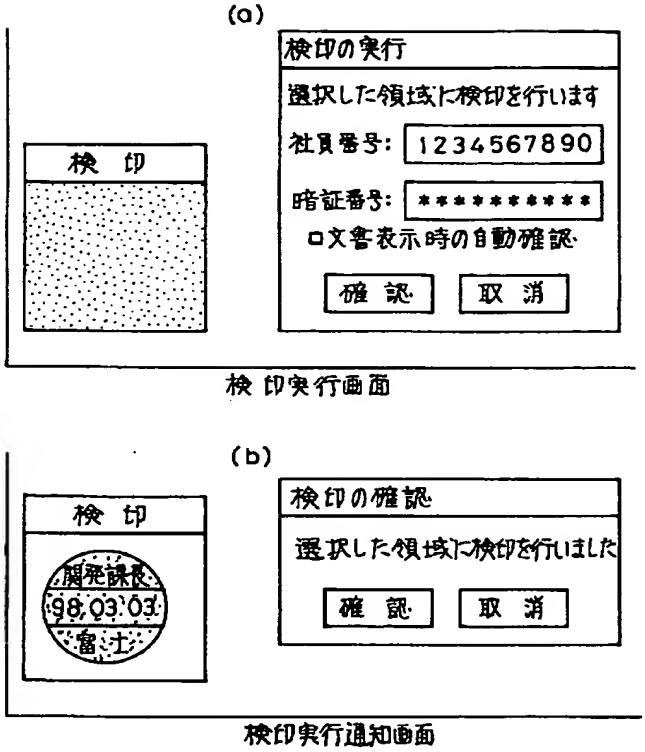
本発明の印鑑イメージテーブル例

印鑑イメージテーブル

社員番号	パスワード	イメージファイル
00001	XXXXXX	印鑑イメージ

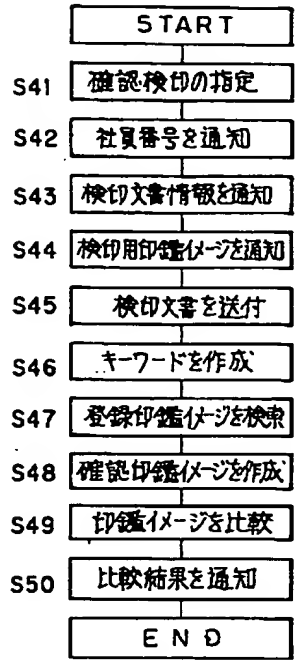
【図７】

本発明の画面例



【図９】

本発明の動作説明フローチャート(その4)



【図１２】

本発明のキーワード組込み説明図

(a)パレットデータ	黒	グレー1	グレー2	グレー3	グレー4	グレー5	グレー6	…
Index	0	1	2	3	4	5	6	
(b)ビクセルデータ	Index0	Index0	Index0	Index0	Index0	Index0	Index0	…

(c)パスワードを「１２３４」
　検印日付を「９８０３０３」
　文書内文字数を「９８０３０２」

(d)キーワード「１２３４９８０３０３９８０３０２」を作成

(e)キーワードを４分割し、定数「1900」「2833」「3090」「4382」

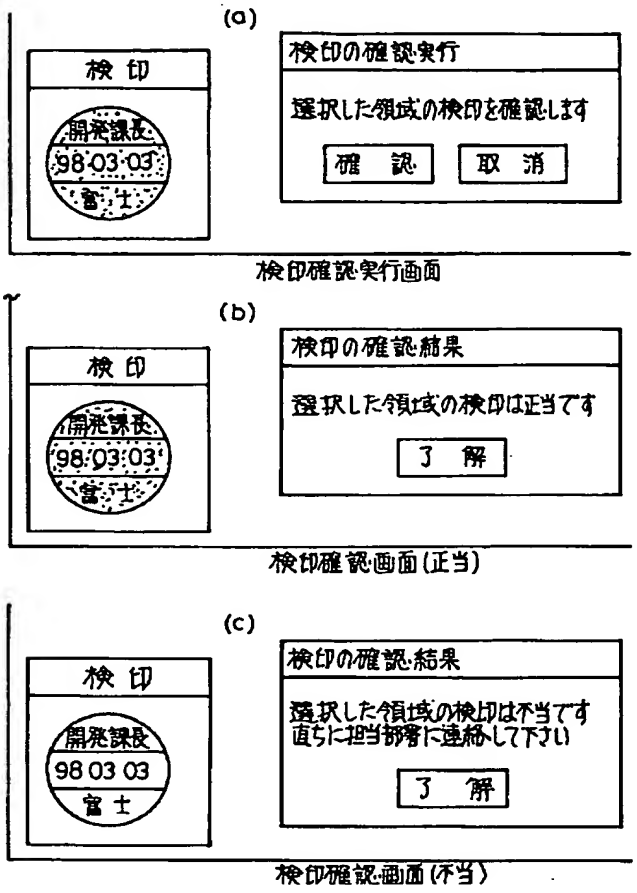
(f)三次曲線を作成

$$Y=1900X^3+2833X^2+3090X+4382$$

(g)$Y=(1900X^3+2833X^2+3090X+4382)\%256$
注)A％B→AをBで割った際の余り

【図１０】

本発明の画面例


(a)
検印
開発課長
98.03.03
富士
検印の確認実行
選択した領域の検印を確認します
確認
取消
検印確認実行画面
(b)
検印
開発課長
98.03.03
富士
検印の確認結果
選択した領域の検印は正当です
了解
検印確認画面(正当)
(c)
検印
開発課長
98 03 03
富士
検印の確認結果
選択した領域の検印は不当です
直ちに担当部署に連絡して下さい
了解
検印確認画面(不当)